REMARKS

Applicants have thoroughly considered the Examiner's remarks in the December 28, 2007 final Office action. Reconsideration of Claims 1-13-15, 19, 20, 23, 30, 32 and 34-38 in view of the following remarks is respectfully requested.

INTERVIEW REQUEST

It appears that the Examiner and the Applicant differ in their interpretation of the prior art and the interpretation of the claims. Thus, Applicants request that the Examiner and the undersigned conduct a telephonic interview to clarify the interpretation of the prior art and the interpretation of the claims. Accordingly, an Interview Request has been submitted simultaneously with this Response.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-13-15, 19, 20, 23, 30, 32 and 34-38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Venkataramappa (U.S. Pub. App. 2003/0188193, hereinafter Venkataramappa) in view of Zhang et al. (U.S. Pat. No. 7,036,142, hereinafter Zhang). Applicants respectfully disagree.

Applicants disagree with the Examiners assertion on page 3 of the action that the claim limitation "the result of in response to the authentication of the user by the second request, the user is authenticated for the first service as a result of the stored first data," merely, as if the client was authorized to access services on a third server in series of subsequent servers, then the client wants to access the first server in the series of subsequent servers, by the SSOToken and the SSOToken to Credential mapping table allows the client to access the first server or any subsequent server based on the third data of the third server (i.e. first data of a first server).

In particular, Venkataramappa teaches a single sign-on authentication method where the client signs on to a first server and in response, the first server generates a ticket. (Page 3, paragraph 55). The first server keeps the ticket and generates and sends a token to the client. (Page 3, paragraph 56- Page 3, paragraph 57; FIG. 3). Next, the client connects to a second server and sends the token to the second server. (Page 4, paragraph 59). The second server requests the ticket from the first server **and authenticates the client based on the token and the ticket. (Page 4, paragraph 60-62; FIG 3).** Therefore, to authenticate the user on the

second server, the second server has to receive the ticket from the first server in addition to the token from the client.

Claim 1

In contrast, claim 1 recites:

> receiving a first request from the first network server to provide the first service to the user;
>
> **storing first data on the client in response to the received first request**, said first data identifying the first service wherein **authentication of the user by the first service is optional**;
>
> allowing the user to access the first service **without** authenticating the user;
>
> receiving a second request from the second network server to provide the second service to the user wherein **the second service requires authentication of the user**;
>
> allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request; and
>
> wherein, **in response to the authentication of the user by the second request, the user is authenticated for the first service as a result of the stored first data**.

For example, the user navigates to a first selected service, namely, Service A, by using a browser of client computer system. (Page 19, paragraph 45). Within Service A, there may be web pages that the service administrator would prefer but does not require the user to be authenticated in order to grant the user access to these web pages. (Page 19, paragraph 46). **In other words, these web pages "desire" authentication from the perspective of Service A but do not require it.** (Page 19, paragraph 46). A "Desired Authentication" cookie (e.g., first data) is stored on the client when the user navigates to Service A to indicate that Service A would like to have the user authenticated, but does not require it. (Page 19, paragraph 48). The cookie is also used by Service A to indicate that Service A has already expressed a desire to authenticate the user. (Page 19, paragraph 49).

Thereafter, the user uses the browser of client computer system to navigate to Service B, which requires the user to be authenticated because it provides personalized or premium content to the user. (Page 19, paragraph 50). As a result, Service B redirects the browser to an Authentication URL of central server and the Authentication URL prompts the user for his or her credentials. (Page 19, paragraph 50). The user submits his or her credentials to central server

and if the submitted credentials match an entry stored in database, then central server obtains a profile associated with the submitted credentials. (Page 19, paragraph 50). **Additionally, the central server also sees that another site, namely, Service A, has expressed a desire to authenticate the user through the "Desired Authentication" cookie.** (Page 19, paragraph 51). The "Desire Authentication" cookie issued by Service A is cleared so that when the user returns to Service A thereafter, Service A will "soft authenticate" the user. (Page 19, paragraph 51). **Accordingly, central server authenticates the user for Service A the next time the user navigates to Service A.** (Page 19, paragraph 55).

Writing for the Supreme Court, Justice Anthony Kennedy observed that a patent claim is invalid for obviousness when the invention combines familiar elements according to known methods to produce no more than predictable results. *KSR International Co. v. Teleflex, Inc.* U.S., No. 04-1350, 4/30/07. However, in this rejection, neither the **element** of **storing first data on the client in response to the received first request, said first data identifying the first service wherein authentication of the user by the first service is optional** nor the **result** of **in response to the authentication of the user by the second request, the user is authenticated for the first service as a result of the stored first data** is found in the combined art.

For at least these reasons, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 1. As such, the rejection of claim 1 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 2-13 depending from claim 1 are allowable for at least the same reasons as claim 1. Claims 22 and 35 have been amended to include similar subject matter as claim 1 and are allowable for at least the same reasons as claim 1. Claims 23 and 36-38 depend from claims 22 and 35. respectively, and are allowable for at least the same reasons as claims 22 and 35

Claim 15

Claim 15, as amended, recites:

> **receiving a first request from the first network server to provide the first service to the user wherein the first service requires authentication of the user**;
>
> authenticating the user for the first service in response to the received first request;
>
> allowing the user access to the first service in response to the received first request;

storing first data on the client in response to allowing the user access to the first service, said first data identifying a first policy group associated with the first service, said first policy group having a shared set of business rules to restrict authentication of a user across different domains;

receiving a second request from the second network server to provide the second service to the user wherein authentication of the user by the second service is optional;

if the second service is associated with the first policy group identified by the stored first data, **allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request;** and

if the second service is not associated with the first policy group identified by the stored first data:

updating the stored first data to identify the second service; and

allowing the unauthenticated user to access the second service.

For example, the user uses the browser of client computer system to navigate to Service B, which requires the user to be authenticated because it provides personalized or premium content to the user. (Page 29, paragraph 65). As a result, Service B redirects the browser to an Authentication URL of central server and the Authentication URL prompts the user for his or her credentials. (Pages 29-30, paragraph 65). The user submits his or her credentials to central server and if the submitted credentials match an entry stored in database, then central server obtains a profile associated with the submitted credentials. (Page 30, paragraph 66). **Additionally, the central server may record the policy group of Service B (Policy Group P) in a "Visited Sites" cookie on the client.** (Page 30, paragraph 66).

Thereafter, the user navigates to a first selected service, namely, Service A which belongs to the same policy group as Service B. (Page 31, paragraph 68). Within Service A, there may be web pages that the service administrator would prefer but does not require the user to be authenticated in order to grant the user access to these web pages. (Page 29, paragraph 64). Since the user has already signed in to a site within Policy Group P, namely Service B, central server will automatically sign in the user to Service A, and an encrypted authentication ticket and profile information of the user will be communicated to Service A. (Page 29, paragraph 68).

Writing for the Supreme Court, Justice Anthony Kennedy observed that a patent claim is invalid for obviousness when the invention combines familiar elements according to known methods to produce no more than predictable results. *KSR International Co. v. Teleflex, Inc.*

U.S., No. 04-1350, 4/30/07. However, in this rejection, neither the **element** of **storing first data on the client in response to allowing the user access to the first service, said first data identifying a first policy group associated with the first service**, nor the **result** of **if the second service is associated with the first policy group identified by the stored first data, allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request** is found in the combined art.

For at least these reasons, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 15. As such, the rejection of claim 15 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 19 and 20 depending from claim 15 are allowable for at least the same reasons as claim 15. Claim 30 has been amended to include similar subject matter as claim 15 and is allowable for at least the same reasons as claim 15. Claims 32 and 34 depend from claim 30 and are allowable for at least the same reasons as claim 30.

Claims 35 - 40 stand rejected under35 USC 103 (a) as being obvious over Venkataramappa in view of Stanko (U.S. Pub. App. 2005/0074126). For the reasons stated above, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 30 such as "**if the second policy group identified by the stored information identifying the second policy group associated with the second service is the same as the first policy group identified by the stored first data, the central server is configured to allow the user access to the second service in response to the received second request wherein the user is authenticated by the central server for the second service in response to the received second request**." As such, the rejection of claim 35 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 36-38 depending from claim 35 are allowable for at least the same reasons as claim 35.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. Applicants thus respectfully submit that the claims as presented are in condition for allowance and respectfully request favorable reconsideration of this application.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Frank R. Agovino/

Frank R. Agovino, Reg. No. 27,416
SENNIGER POWERS
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

FRA/BAW/cjl